A FORMULA FOR CONSTRUCTING MIGNOTTE SEQUENCES

MAREK PUTRESZA

Abstract. We present a new, direct and simple formula for constructing Mignotte sequences.

One of the secret sharing schemes is the Mignotte threshold secret sharing scheme, which uses the Mignotte sequences, defined as follows.

A (k, n)-Mignotte sequence, where $1 < k < n$ are integers, is an increasing sequence

$$m_1 < \ldots < m_n$$

of pairwise relatively prime positive integers such that

$$\prod_{i=1}^{k} m_i > \prod_{j=n-k+2}^{n} m_j, \tag{1}$$

i.e., the product of the smallest k terms is greater than the product of the $k-1$ largest ones. To ease the notation, put

$$M = \prod_{i=1}^{k} m_i,\ N = \prod_{j=n-k+2}^{n} m_j.$$

Additionaly, we require the quantity $\frac{M-N}{N}$ to be big.

The known method of constructing Mignotte sequence (see e.g. [1], page 9) is indirect; it relays on finding special intervals with sufficiently many prime numbers. In this note we prove the following theorem, which provides us with a direct and simple formula.

Theorem 1. *Let $q_1, \ldots, q_n$, $n \geq 3$, be an increasing sequence of pairwise relatively prime positive integers. Define:*

$$P = \prod_{1 \leq i < j \leq n} (q_j - q_i) \tag{2}$$

Then

$$P + q_1, \ldots, P + q_n \tag{3}$$

is a (k, n)-Mignotte sequence for any $1 < k < n$.

Proof. First we check that (3) are pairwise relatively prime numbers. Compute for any $i < j$

$$\gcd(P + q_i, P + q_j) = \gcd(P + q_i, P + q_j - (P + q_i)) =$$
$$= \gcd(P + q_i, q_j - q_i) \stackrel{\star}{=} \gcd(q_i, q_j - q_i) = \gcd(q_i, q_j) = 1$$

where the equation marked $\stackrel{\star}{=}$ is valid since $q_j - q_i$ divides P.

Now we check that the condition (1) is satisfied, i.e.,

$$\prod_{i=1}^{k} (P + q_i) > \prod_{j=n-k+2}^{n} (P + q_j). \tag{4}$$

We analyse the case for $n = 3, k = 2$ separately. We will show that a stronger inequality

$$(P + q_1)^2 > P + q_3 \tag{5}$$

is satisfied. Rewrite it as

$$P^2 + P(2q_1 - 1) + {q_1}^2 - q_3 > 0. \tag{6}$$

Define the polynomial

$$f(x) = x^2 + x(2q_1 - 1) + {q_1}^2 - q_3.$$

We will show that inequality (6) is valid by proving that P is greater than any root of f. Compute the discriminant of f,

$$\Delta_f = (2q_1 - 1)^2 - 4({q_1}^2 - q_3) = 4q_3 - 4q_1 + 1 > 0.$$

The larger root of f equals

$$\frac{\sqrt{\Delta_f} - (2q_1 - 1)}{2}.$$

We will show that

$$q_3 - q_1 > \frac{\sqrt{\Delta_f} - (2q_1 - 1)}{2}. \tag{7}$$

Indeed, transforming (7), we get the following equivalent inequalities

$$2(q_3 - q_1) + (2q_1 - 1) > \sqrt{\Delta_f}$$

$$2q_3 - 1 > \sqrt{\Delta_f}$$

$$(2q_3 - 1)^2 > \Delta_f$$

$$4(q_3)^2 - 4q_3 + 1 > 4q_3 - 4q_1 + 1$$

$$q_3(q_3 - 1) > q_3 - q_1$$

The last inequality is valid since $q_3 > q_1 \geq 1$. Thus (7) holds, and we are done, since $P \geq q_3 - q_1$.

Now we prove (4) in general case $n \geq 4$. Factoring out P, and then dividing by P^{k-1}, we get the following equivalent inequalities

$$\prod_{i=1}^{k} P(1 + \frac{q_i}{P}) > \prod_{j=n-k+2}^{n} P(1 + \frac{q_j}{P})$$

$$P^k \prod_{i=1}^{k} (1 + \frac{q_i}{P}) > P^{k-1} \prod_{j=n-k+2}^{n} (1 + \frac{q_j}{P})$$

$$P \prod_{i=1}^{k} (1 + \frac{q_i}{P}) > \prod_{j=n-k+2}^{n} (1 + \frac{q_j}{P}). \tag{8}$$

To prove (8), we will show that a stronger inequality

$$P^{\frac{1}{k}}(1 + \frac{q_1}{P}) > (1 + \frac{q_n}{P}) \tag{9}$$

is satisfied. Transforming it, we get

$$P^{\frac{1}{k}}(1 + \frac{q_1}{P}) - (1 + \frac{q_1}{P}) > (1 + \frac{q_n}{P}) - (1 + \frac{q_1}{P})$$

$$(P^{\frac{1}{k}} - 1)(1 + \frac{q_1}{P}) > \frac{q_n - q_1}{P}$$

$$P(P^{\frac{1}{k}} - 1)(1 + \frac{q_1}{P}) > q_n - q_1. \tag{10}$$

We have $P \geq q_n - q_1$ by (2), and obviously $(1 + \frac{q_1}{P}) > 1$, since both q_1 and P are positive. Thus, to prove (10), it remains to show that $P^{\frac{1}{k}} - 1 > 1$, i.e., that $P^{\frac{1}{k}} > 2$. Since the sequence $q_1, \ldots, q_n$ is increasing, we get for any $n \geq 4$

$$P = \prod_{1 \leq i < j \leq n} (q_j - q_i) \geq \prod_{1 \leq i < j \leq n} (j - i) = \prod_{i=1}^{n-1} i! > 2^{n-1}.$$

Hence indeed

$$P^{\frac{1}{k}} > 2.$$

□

Remark 2. Note that the procedure given by Theorem 1 can be iterated as many times as one wishes. If the procedure is applied t times, the resulting numbers are

$$tP + q_1, \ldots, tP + q_n,$$

which asserts that the quantity $\frac{M-N}{N}$ can be as big as needed. Indeed, for t large enough we get

$$tP + q_1 \approx \ldots \approx tP + q_n,$$

so

$$\frac{M - N}{N} \approx tP + q_1 - 1.$$

The P itself is large, since

$$P > \prod_{i=1}^{n-1} i! > e^n$$

for $n > 4$, where e is the base of the natural logarithm.
Observe that finding an initial sequence of pairwise relatively prime positive integers is a very easy task; consider for example the following elementary proposition.

Remark 3. Let q_1 be a positive integer. Then the terms of the sequence defined recursively by

$$q_{k+1} = 1 + \prod_{i=1}^{k} q_i$$

are pairwise relatively prime.

Acknowledgements

The author acknowledges the support from BESTStudentGRANT 119/39/UAM/0010. Words of gratefulness goes to Stefan Barańczuk for proposing Theorem 1 and the supervision. Special thanks go also to Tomasz Kościuszko, as an inspirer of our participation in BESTStudentGRANT program. Lastly, we address acknowledgment to Aleksander Tytus for discussions over the cryptographic side of this project, as well as suggestions which lead to simplification of the proof.

References

[1] E. Kranakis, *Primality and cryptography*, Wiley-Teubner Series in Computer Science, Wiley, Chichester, 1986 Teubner, Stuttgart, 1986; MR0846010

Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Poznań, Poland